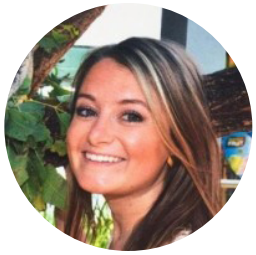
Rethinking Your Approach to Enterprise Risk Management

WEBINAR TRANSCRIPT NOVEMBER 2019

Dataminr®



Krista Worley

Account Director, Corporate Risk

Dataminr

Michael Gladstone

Senior Manager, Emergency Management & Planning

WeWork

Michael H. Gladstone is The We Company's Senior Manager, Emergency Management & Planning and is one of the longest tenured members of The We Company's security team. He is responsible for the development and implementation of The We Company's Global Crisis and Emergency programs, runs the corporate Emergency Management Team, and manages programs with the aim of protecting employees and members. Michael has previously worked for the U.S. Department of State as a Crisis Management Program Officer and for the New York City Department of Education as a High School History teacher. He holds a M.A. in International Law and Global Security from Georgetown University, a M.A. in Teaching of Social Studies from Columbia University, and a B.A. in History from Brown University.

Scott

Good afternoon and welcome to today's webinar, Rethinking Your Approach to Enterprise Risk Management, presented by Security Management Magazine and Dataminr. Security Management Magazine is the industry standard for security leaders and is sent to all ASIS members. Dataminr is recognized as one of the world's leading AI businesses. The company's clients are the first to know about high-impact events and emerging risks so they can mitigate and manage crises more effectively.

I'd like to introduce today's speakers. Michael H. Gladstone is The We Company's Senior Manager, Emergency Management and Planning, and is one of the longest-tenured members of The We Company's security team. He is responsible for the development and implementation of The We Company's global crisis and emergency programs, runs the corporate emergency management team, and manages programs with the aim of protecting employees and members. Michael has previously worked for the U.S. Department of State as a crisis management program officer and for the New York City Department of Education as a high school history teacher.

Next, I'd like to introduce Krista Worley. Krista has worked in risk management solutions for the last eight and a half years, and for the last two, she's focused on crisis communications in social media. Krista has worked with numerous financial institutions and corporate entities on how to capture relevant content, breaking information, and threats.

And with that, I will turn it over to Michael and Krista.

Krista

Thanks, Scott, and thank you all for taking the time to participate in this webinar today. Today's conversation will address Rethinking Your Approach to Enterprise Risk Management. A quick look at our agenda: WeWork organizational structure, risk at WeWork, mitigating risk, unifying across the enterprise, measuring risk, resources for risk management, and questions. Our session today should run no longer than one hour, with plenty of time reserved at the end for as many questions as we can take. If we cannot address all of your questions during the hour, we'd be happy to answer them through email or a call afterwards.

Let's go ahead and dive in. Despite their best efforts, many companies lack an appreciation of the spectrum of risks they face. Depending on the type of risk a company identifies, one or more departments assume responsibility for managing it. Even in the most sophisticated organizations, companies lack a holistic view. This puts the C-suite in a precarious position since they rely on the departments that report to them to understand and mitigate risk collectively. Risk does not always sit neatly within a company's organizational chart. Some risks impact more than one department, and if a risk does not fit into a department's mission, it can go unaddressed. When a crisis hits, an enterprise with blind spots may struggle to find and address them. Departments unaccustomed to working together may struggle to do so. Corporate risk impacts many functions across an enterprise, and executives need to embrace an enterprise-wide view of risk, not just as it pertains to their function.

So Michael, how is WeWork structured, and who is responsible for risk?

Michael

Well, thanks, Krista, and thank you to Dataminr for inviting me here today. I'll talk a little bit first about WeWork so that everyone on the call knows who we are and what we've done. WeWork has expanded greatly in the last nine, almost 10 years,

that we've been in existence. For perspective, I joined in July of 2016, and we had less than 100 locations globally and less than 1,000 employees. Now, in 2019, we've got over 10,000 employees, over 500,000 members, 900 locations scattered around 150 cities in 36 countries, and over 51 million square feet of space, co-sharing and otherwise.

Putting that in perspective, our enterprise risk has continuously grown over the last number of years, and because of that, as we saw on the previous slide with risk organizations, we actually have a very dispersed risk profile. We don't have one team that is covering all of the risks. We have crisis communications where our public affairs teams are working inter-departmentally and intra-departmentally to address things both internally, through the press, and on social media. We have my team, the emergency management team, which sits in our global security department, and we also have a business continuity disaster recovery team who is also addressing those risks.

Risks can be both physical, so the emergency management team and business continuity team. We have cyber-risk and just general technology and systems risks, our business continuity teams and our information security teams are involved with that, an entirely different division then to themselves. We've got, obviously, risks to our employees and our members, so we have crisis communications, emergency management working together. We also have health and safety risks. Doesn't matter who that person is, but if a wire is on the ground and someone trips, we need someone to take care of that, too. All of this encompasses brand and reputational risk because if something can go wrong on the physical side, it could negatively impact our brand. We have a lot of different departments, but the key is that we all work together, and we all talk with one another when a crisis or risk appears.

Krista

Thanks for the context. It's definitely a lot, and so given that, what are the biggest risks to your organization now, and three years' time, and how do you plan to mitigate them?

Michael

I think the biggest risk that we have, first and foremost, employee and member safety. That is our top goal is to ensure that our members, our 550,000 plus members, all the guests that they bring into our spaces, and WeWork employees are safe. We have people in our spaces 24/7, so we need to ensure that everyone, regardless of where they are, regardless of what time they are in our space, that they're safe. So that's our first concern all the time.

Secondly, we're also concerned with brand reputation because if any of the crises that have happened globally impact our brand, we need to be able to confront those head-on and do that as quickly and expeditiously as possible. A lot of folks on the webinar today might not necessarily be a part of the marketing department or be a part of the crisis communications or public affairs departments, but even as a security professional, you have to be thinking about how can this particular risk impact our brand as an enterprise.

Third thing would be travel and bleisure, and for those who are on the call, don't worry, we'll explain what bleisure is. WeWork is a very large company, like I said, 10,000 employees over 36 countries. We have people everywhere. We're constantly opening up new locations. You can't have the kind of explosive growth like we've had without consistently opening new businesses and new communities, as we call them. So we have people traveling all the time across the globe, and because

we have that "sun never sets" model, people might be flying into a protest in Hong Kong or in Chile. They might be transiting a country that's having a coup. Luckily, no one's in Bolivia this week, but that could happen, right? There might be other socio-political issues that are happening, and we need to make sure we know where all of our employees are. At the same time, we have a very Millennial-centric company, and there's this new term out there called bleisure.

Bleisure is when you combine business travel with leisure. What we have seen is that a lot of companies today are offering incentives for employees, which does increase risk, to say, "If you go on business travel, we also will give you time to explore the city we're sending you to," or a lot of people say, "I'm going to somewhere in Europe that I've never been before. Why don't I take some of my PTO and also explore countries near where I'm going, instead of having to spend some of my own money, traveling there at another time." Great example of how this has impacted WeWork was in 2017, we had some colleagues traveling in Southeast Asia for work, and they decided, "Well, we're close. We'll go to Bali and enjoy the awesome beaches there." Lo and behold, the volcano in Bali went off, and suddenly we had employees, who we didn't know were there, because they were in a different location, suddenly they're coming to Bali, and now they're stuck. So we had to deal with that as well.

Finally, and I think this really impacts any business, doesn't matter what business line you're in, but environmental concerns and severe weather. We are constantly seeing things like earthquakes occurring on a global scale, but at the same time, we also have wildfires in the West that are impacting the air quality in our cities where we have locations, or we have winter storm season rolling around. Hurricane season, this year, was not as bad as it has been, but they're constantly getting worse and worse each and every year.

These are the biggest concerns, and while these are concerns today, in three years' time, they're probably going to remain our core focus. But as we'll talk about a little bit later, the geopolitical changes that are going to happen in the next one, two, 12 years, we can't predict what's going to occur, and those are probably going to be shaping how we address enterprise risk as well.

Krista

Definitely, and thanks. While it's impossible to identify and mitigate every type of risk, an inability to identify risk and develop contingency plans results in blind spots. A blind spot may develop when individual departments lack adequate solutions to gather data fast enough to meet the needs of the organization with respect to risk management. Where have you found blind spots in identifying risk, and how did your organization react to ensure these gaps were covered moving forward?

Michael

It's a great question. I think the first thing that we've always, and regardless of what business I've been in, or when I talked to my colleagues, the first thing that everyone always says is the biggest threat to enterprise risk is how do you respond to the unexpected? For example, everyone says, "Okay, there's going to be earthquakes on the West Coast," but until recently, the seasonal wildfires that happened in California, didn't have as big an impact as they have had on places like San Francisco and L.A. until the last two years. But now that's a standard. We had to react to the unexpected smoke billowing hundreds of miles and getting into our buildings, and we can't just say, "Okay, that was a one-off event, and we're never going to deal with it again." Responding to the unexpected means that you have to have planned and preplanned for all potential eventualities. Being really proactive about what you know is going to occur and planning for the unexpected that you say, "Well, this

will never happen to us," that's the time when you, as an enterprise risk team, need to sit down together and start being proactive about those risks. It could be active intruders. It could be natural disasters. It could be economic collapse. People have to start planning well in advance because if you can put that risk mitigation strategy in place, those blind spots start becoming visible. That's really the key.

Krista Great. I mean, I agree. If departments involved in risk management rarely work together, until there is a crisis, arguably those blind spots do exist.

Michael Totally.

Krista Corporate risk is evolving, and in order for enterprises to ensure they are detecting and mitigating against risks appropriately, they must identify blind spots across the organization and take a unified approach to addressing those gaps. How do you unify different categories of risk across the organization, physical security, cyber-security, brand awareness?

Michael We take, what I like to call, a mobilized approach. We are, as I mentioned, diverse in many different risk teams, but those risk teams are constantly in communication and using a variety of technologies, which we'll talk a little bit about later, to help address those risks. We aren't stuck to, what I like to call, the plan on a page. We are utilizing technology to allow us to take that plan on the page, to then exercise that plan on the page, and then when a crisis or risk does appear, we then work proactively and interconnectedly to address that risk.

We're also taking all those different risk categories and saying, "Okay, at the same time that there might be a cyber or an information security risk, there can also be a physical security risk happening at the same time." I think natural disasters are a great example of that because it's possible, in a natural disaster, that all of your various, different risk groups, business continuity, disaster recovery, information security, physical security, risk management, or emergency management, or crisis management, whatever you call it, and public affairs crisis management, are all going to be impacted at the same time. How we unify that is to make sure that there is a free flow of information going as high up as possible on the chain and as low down as possible because you never want to silo the information. Enterprise risk folks have a great wealth of information that they get. Don't silo it. You want to make sure that you're sharing. Unless it's very sensitive information, share all the data during a crisis as is allowed and possible. Of course, your legal department might have something to say about that, and that's fine too, and that's important. You want to also work with your legal teams, but you want to make sure that everyone is working on the same information at the same time.

Krista Perfect, and you mentioned a mobilized approach. Mobilizing an appropriate response to risk requires communication across the enterprise, and I know you mentioned that. How have you mobilized the approach? What are some examples of success in your mobilized approach?

Michael Yeah, I think some of the most difficult emergencies and crises that we have faced have been things like natural disasters that have a broad impact on a broad number

of people, simply because when we practice and have our emergency management teams taking that, like I said, mobilized and unified approach, they are not necessarily practicing for a real-world scenario, where they are in different places at different times. And so we have to make sure that we're planning for, at the end state, when there is a crisis, how are people going to efficiently and effectively react?

I think one of the best examples where we've had to implement the mobilized approach for "You're not all going to be in the same room. How do you react?" would be the Mexico earthquake in 2017. That was a great example. Why? Because at the time the earthquake struck, our leadership team was in a variety of different places around Mexico City. They all had to come together eventually, but in that immediate aftermath, they were dealing with multitudes of different issues, health and safety of their employees and of the membership. They were dealing with health and safety of their families and their homes. They were dealing with, "How do we physically get from one location to another?" And because of the fact that we started and prepared for a mobilized approach, utilizing technology to help us get better at risk management, we were able to start linking people together through technology to address the issues, while at the same time, being very cognizant that we didn't have every player that we usually had involved in responding to the crisis. We did our best, and we were able to maintain a good awareness of how our brand was impacted by the crisis, how our people were impacted, how our members were impacted, and how our physical locations were impacted. I think that's one of the best examples of a mobilized approach.

We also have had really good examples recently where different parts of the teams, for example, just this week, we have locations in Israel, and we have our member communications team dispersed around the globe. Through utilizing technology, even though we all have the same crisis management plan, we don't have to physically be in the same place. In this particular instance, we had the emergency management team in New York linked up with the emergency management team for Israel, linked up with our member communications team in the UK, all focused on one issue.

Krista

You mentioned this earlier as well, but the managing risk in silos is often rewarded in the form of departmental goals, at the expense of overarching goals that cover the entire enterprise. How do you measure successful risk management?

Michael

I think one good thing before I address the issue of managing successful risk management and what that looks like, would be, Krista, to address the issue that you talked about, siloing. Yeah, we all love to achieve things as a department. We want to show our superiors that our department achieved something really great. But if only your department achieves something really great, and the risk has multiple people impacted by it, if your department is the only one that succeeded, and you have a ton of great information and resources and tools to give to the rest of your risk partners, but you didn't do it, you've already failed out of the gate.

But what are we talking about with successful risk management? I think the first thing is that no one gets hurt during a crisis. Oftentimes, that's not realistic, but you want to make sure that you are doing everything you can to limit the amount of damage to individuals that's happening during a crisis. If you're working proactively before a crisis occurs to limit the health/life safety risk to your employees, to your members, to your customers, you are being successful in mitigating risk.

The second thing would be to ensure that you have sound infrastructure. We oftentimes get laser-focused on making sure that the people are okay, but your assets are just as critical. Everyone can be fine, but if the building itself, if your asset is something that can't be occupied for months on end, how is that going to impact your brand? How is that going to impact your ability to deliver your product, whatever it might be, to your particular clients? So you have to make sure that, "Okay, health/life safety, first and foremost." We've had discussions before about this, you and I, but health/life safety is always the first. Doesn't matter what kind of a security professional you are.

But the second thing you always need to think about is how are we planning and ensuring that our infrastructure is sound? Is it that we have redundant sites, cold sites, warm sites? Is it that we have evaluated relocation plans, tested those plans, and when I say tested, I mean physically gone out, tried to do what you said you would do, and not on an off-hour, right? Because emergencies never, ever happen at two in the morning. They happen in the middle of the day. So have you driven that relocation or evacuation route?

And then, especially at WeWork, we're focusing on what has, or how can we, I should say, have the least amount of impact on the following things- our members' experience. On the backend, things might be crazy, but as it goes back to the idea about brand reputational risk as well as keeping a consistent product, things might be happening on the backend. The risk teams might all be spun up, but if there's a very low impact to your customer base, in our case, our members, then we've succeeded. If, even if, during a crisis, you don't smell squeaky clean, but at the end your brand comes out on top because of how you were proactive in addressing a crisis, if you are able to help the community that was in crisis during that particular incidence, then you've actually succeeded at risk management.

And last, but not least, is continuity of operations. People might get hurt. It's a reality of the situation. Infrastructure might get damaged and can't be occupied. That's a definitive reality. But if you have executed good, cross-functional risk plans, can move people from one location to another, send people to telework, send people, whatever it is, you can utilize technology to ensure that you have continuity of operations, you've successfully mitigated risk. I think before we move on to the next topic, I'd love to point out that I'm not saying that there won't be bad things that happen, right? There are always going to be risks, and sometimes a few eggs might get broken, but it's important that you overcome those, what you might see as challenges or deficiencies, you overcome those issues in order to ensure that, holistically, all the right players are working together and that your brand, your continuity of operations, and your people are as safe as possible. That is successful risk management.

Krista

Great. When we're talking about those instances that we know will inevitably happen, an organization's response may lag events by a significant margin, worsening the incident, creating additional risk, and inflicting incremental losses on the business. What ROI do you look for when applying an emergency risk management plan to your organization?

Michael

I think that's a great question. My team's ethos is when there's this tiny little kernel of a crisis, we jump into action. People might say, "Oh, you're being hyperreactive." Well, listen, that happens sometimes, of course, but the case that we're trying to prove is that if we start reacting sooner to a potential crisis, we mitigate those risks,

and like we just talked about, you become more successful with risk mitigation.

So the ROI that we're looking for is not necessarily the amount of money that we save the enterprise or that we successfully grew our quarterly earnings. That's not the risk manager's top priority. Instead, it's not quantitative, it's more intangible, right? It's more about thinking, "Okay, if we prevented this particular crisis from being as bad as it could've been, maybe," in the WeWork case, "we say, 'Okay, we've got more members who are coming back the next month because they were happy with the lack of interruption to their business.'" Or an enterprise-level client is going to be able to make a big sale because we can say, "Look, we can't prevent a risk from happening, but here's how the WeWork risk teams address this issue."

You can't always argue that there are specific numbers that are going to make you successful in a crisis, and unless there's one specific technology risk, because obviously, if the Internet goes down at WeWork— we're sitting in a WeWork location right now— if the Internet goes down, that doesn't look good for WeWork. Not saying it has, but if that happens, and that we can monetize because we can say, "Well, our members are dissatisfied. We've had to give discounts," whatever it might be. It's oftentimes, difficult in things like a natural disaster to see what you saved or you didn't lose in a monetary fashion. So again, it's really, to me, risk management has an ROI that's not self-evident, if at all. It's very difficult sometimes to make that corollary. It's hard for non-risk management people to understand when we say, "We don't know the exact impact that this bit of technology or this plan will save us." It's very hard to quantify, and that's a challenge for a risk management team.

Krista

Definitely. Thanks, Michael. While internal audits, or an enterprise risk function, may attempt to look across the enterprise to ensure the appropriate risk ownership and mitigation exists, they may lack the ability to bring about change. Often organizations lack sufficient justification to make a change in how they manage risk. Even if an organization operates with a broad definition of risk in mind, it often lacks the tools to test or validate their theories.

Michael

Yeah, that's really, really important.

Krista

Yeah, and what they cannot see, they cannot manage, nor justify the resources to do so. Nevertheless, whether managed or not, risk can manifest as an incident at any time. Additionally, some enterprises may possess a firm grasp on risk as it stands currently, yet lack the ability to evolve their resources to emerging types of risks. What resources do you deploy to address risk?

Michael

I think that the biggest thing that we utilize, and that I find really proactive and really good risk management teams are using these days is technology. There's oftentimes a fear in the risk management field or in the security field about utilizing technology. Technology, however, is going to give risk management and enterprise risk teams an edge over their competitors who are relying solely on just the knowledge within your heads. Technology helps us supplement what we have built, our knowledge base, for years and for decades, and makes us that much faster because, in my estimation, risk needs real-time information. When there's a risk out there, you want to know before anybody else knows, what the next evolution of that crisis is, and so you want to have things that are not just a static resource like that plan on the page. Your ROI and this goes back to the question you just asked is that your ROI for risk is

technology helps you to respond faster, and so you then mitigate the impact to your business. So the end result here is that you have much faster crisis response. You can get that message out to your clients that much quicker. Sometimes, obviously, you have to be wary, right? If you send out a message so fast and everyone's talking, "Well, what are they discussing? We don't know about this crisis." You have to obviously give people the right information at the right time, but instead of being two hours behind the ball, you're right on the money, you're doing a lot better.

When you spin the idea of investing into risk management, you don't want to say, "Listen, being a risk management and giving us technology, yes, we're a loss leader." Instead, you want to say that you can prevent loss from happening, you may not be able to quantify it, but prevent risk from happening by investing in technology. I think one of the things that I really love about using technology like Dataminr and other traditional intelligence services is that if a risk team, whether it's emergency management, business continuity, if you can just be like 15 minutes ahead of the curve during an event that's impactful to the business or people's health/life safety, you're also showing your return on investment right there.

I'd love to bring up a specific example where we just recently were ahead of the curve by using technology. That was the hijacking scare, as it were, we'll put that in quotes, in Amsterdam. For those who aren't fully aware of what we're talking about, so earlier this month, there was a report of a purported hijacking at the Schiphol Airport in Amsterdam. Literally, the plane was on the ground, and we got an alert from Dataminr, and within minutes of that alert coming out, our intelligence team was checking multiple different sources to cross-verify the information. Our team was jumping onto our travel management tool to check, "Did we have any travelers," okay, going back to that idea, "What are our biggest risks?", right?

Krista

Okay, right, right.

Michael

We suddenly have travelers at risk because there's a crisis at an airport, checking all of our travelers' statuses. Luckily, we didn't have anyone in the airport at the time, and no one was transiting until the next day, but we were able to look at all of that information, start talking with our teams relating to public affairs because even though we don't have locations at Schiphol Airport, this could have a ripple effect on our members, because we do have locations in Amsterdam. A lot of time, people hear things on the news they wonder, "How is this impacting us?" and if people are in our space, they want to know that we are on top of that particular issue.

So Dataminr gives the alert really quickly, and suddenly, 15 to 20 minutes later, the information appeared in various traditional intelligence sources, as well as in the media. But in those ensuing 15 minutes, we had already done all the proactive work that we needed to do to understand what is the potential risk to WeWork employees and to our business line, and notified all of the other risk teams to say, "We don't know what's happening, but here's what we know right now." Obviously, in the end, as all of this turns out to be a false alarm, which is great, but we were already putting ourselves in a position to address that risk by utilizing technology.

We've also utilized technology to address risk by simulating, in a much more realistic way, crises and emergencies on interactive platforms, which allow us, and it goes back to the mobilized approach we were talking about earlier, allows us to take people across the globe, put them into the same simulated environment, which is really great because we can create fake newspapers. We've taken Dataminr alerts,

tweaked them, and made sure that they look slightly different than reality, but they look realistic to the people receiving them. We can create fake emails so that it looks as if people from up top are sending requests down to various teams across the globe. And much like any true tabletop exercise or any true crisis, I should say, we start injecting as the crisis itself is evolving, we inject things that weren't preplanned into the exercise.

It's really cool to allow us to have that technology, because when you do a plan on a page, everyone sits in the room and they say, "Well, we'll do X, Y, and Z." Technology allows us to force various different groups to actually run through their checklists, to actually state how they're going to achieve the end result that they want to do. What I really love is that, as a security professional, we have all this great knowledge, all those crises and emergencies you've gone through, all the courses that you've taken, you can now apply that knowledge and use technology to make you even better. It really shows your higher-ups that you're thinking outside the box, you're not just thinking, "More knowledge?" You're thinking with all these great tools that you have at your disposal.

Krista

Right, and you've talked a lot about technology. What do you see the role of AI being in risk management in the future?

Michael

I think that AI is never, ever going to replace the analyst, the person reading the information on the backend. But like I said before, it's going to help you, as a security professional, shine because technology enhances the depth of your knowledge. So, for example, right now, we're tracking protests in Chile as I am sure a lot of people are, whether you're using Dataminr or another tool, but it's difficult to see how every new Tweet or social media post is being used by various different groups. When using a tool like Dataminr, or any AI tool, it allows machine-learning to help you as a risk professional, to act even faster and really, and not just faster, but react smarter.

Let's talk reality for a second. Hashtags consistently change. Someone changes the way it's spelled, someone gets word that the authorities are tracking that hashtag, so they change the hashtag. Unless you have an unlimited number of people on your team, you're not going to be able to troll social media and find all that information, but if you use something that has AI behind it, and it learns about what you, as a risk professional, care about, then you have this much stronger tool beside you because you don't have to worry, "Will the topic change? Will the hashtags change? Will the phrasing that people use change?" Let the AI help you.

And additionally, I think this is really important, and I learned this even more so now working at WeWork than I ever did before, I don't know every language that's out there, right? We support 36 different countries. We have a multitude of languages, and it's likely that our colleagues who are on the webinar right now, they don't know every language out there either, and their team probably doesn't know every language. If you have a team that covers every language that you're in, you are in a golden position, by the way. So AI is going to help you decipher important information that's otherwise going to have to have you either pay a translation service or have your team translate, which can take a lot of time. It's great to use technology, but if the technology doesn't help you understand what that information is, it doesn't matter if it's 15 minutes in advance. When using AI, you not only know early, but you know the information correctly.

So my thing is, I think AI is going to continue to make risk management much

easier and more efficient, and it should be embraced because it's the only way risk professionals can make AI work for them. If you embrace the technology, not as, "Ooh, this could make me lose my job," but help me enhance my job, you are going to be able to evaluate those technologies, utilize them, and encourage, and I would say, even force the providers of that AI technology to make the product work for you. So I really encourage all risk professionals, embrace technology. Of course, you have to be within budget and what have you, but embrace technology. Get to know AI providers because risk professionals out there, I'm telling you, it will revolutionize in a really great way, how you can approach a crisis or an emergency.

Krista

Thanks, and kind of going back a little bit earlier, you mentioned some scenarios where you were playing out tough cases and acting upon those. One of the ways to test a company's ability to mitigate risks is to determine whether a contingency plan exists for a certain type of risk. Some may argue that the black swan theory holds true, meaning certain incidents are impossible to predict and manage. While that may be true for certain events, upon closer inspection, seemingly unpredictable events may highlight knowledge deficiencies and a lack of the suitable tools to bridge the gap between what a company knows and needs to know, rather than a black swan event.

Michael

Yep.

Krista

What is a bad day from a risk perspective?

Michael

Ooh. That's definitely a loaded question. I think a bad day, three things can happen, right? The first is that if there is some kind of a life safety issue that any part of the risk enterprise team could have prevented from happening, but it happens, that's a bad day. Doesn't matter what the risk is, if someone is injured or, god forbid, there's a fatality because of something that your team knew was a risk and wasn't proactive about, regardless of cost, the negative ramifications of that, that could be immense. So that's the first thing that comes to mind.

I think another thing that comes to mind is if there is an impact to your brand. Not necessarily the people or your customers, but the brand that you knew was out there, and you didn't do anything about it because you said, "Well, maybe someone else is dealing with this," or, "That doesn't sound like it's going to be really a big thing," that's a bad day for risk management. Not being proactive about protecting your brand.

And then, I think, even the most impactful thing is when your superiors come to you and say, "What is happening here?" but you have no idea what they're talking about. That's a really bad day for a risk management professional because either the resources that you have chosen to use have failed you, or you're sort of left standing there with that look on your face like, "I am not qualified to be in this position." A risk management professional's ultimate goal is like we've talked about already, being ahead of the curve. If your superior or a C-suite comes and asks your superior the question, they should already have the answer because you have figured out, "This is a risk. I need to let somebody know, and here's how it's a risk. Here's how we can mitigate it." Don't wait for the question to be asked. Be proactive, and that's how you avoid the bad day because that bad day will happen if someone says, "Why didn't we know about this risk?" and you don't have a good answer.

Krista

Thanks, and you mentioned kind of letting someone know that something was happening, or someone letting you know something was happening. How is information communicated across the WeWork organization when the company is hit?

Michael

Yeah, it really goes back to this idea that there has to be a free flow of information. It has to be utilized through technology. It has to be utilized in person. And when I say technology, it doesn't have to be the greatest thing under the sun. It can be as simple as picking up the phone and calling someone because that looming crisis that you think isn't going to become a problem is probably already a problem that you just don't know. So you have to make sure that everybody is informed, even if you don't think that the public affairs team needs to know about crisis, don't make that judgment yourself. Share that information. Allow that particular team to judge whether or not they need to be involved at the outset. And all avenues of communication must, and I never am insistent about things, but please, must be organized before your crisis occurs because that crisis could actually impact your modes of communication. That could impact how you share information, and if you haven't thought through all the possible scenarios beforehand, you're putting yourself in a weaker position.

Krista

Okay. Last question before we move into the Q&A portion of the webinar. What is the one thing you think will change in the next 12 to 18 months that will impact and affect risk?

Michael

Ooh. Wow. I'm going to go with a very broad topic, but I think it's really applicable in the last four or five months and will be for the next 12 to 18. It's geopolitical risk. Right now, we're tracking issues in Hong Kong, Chile, Bolivia, Venezuela is consistently moving there. We're tracking issues in the Middle East. It could be general unrest like we've seen in all those particular instances. It could be things like Brexit. We don't know what will happen, and also that uncertainty of what's going to happen impacts the business. The 2020 election in the U.S. could have a dramatic impact. We don't know how. And because we don't have an idea about what will definitively happen, if we had a crystal ball, it would be amazing. But we don't. So the ability as risk professionals to plan for all these particular unknowns is really difficult. Those are the biggest things. Geopolitical risk of any stripe. We know that storms and natural disasters are going to happen. We know that those things are getting worse. What we don't know is how will governments, how will people react to all kinds of different socio-economic pressures, and that's the thing that really keeps me, my team, and a lot of other people up at night.

Krista

Right. Michael, thank you so much for your time and insights today, and we will now open it up to questions.

Scott

So we're going to jump in with a question for Michael. It's really if you can explain your department. How many people work in your department, how you interact with other departments, I mean, what is kind of the role of the emergency management and planning department at WeWork?

Michael

It's a great question. So our team has evolved over the last three and a half years.

There was no emergency management team in the past, and this team has evolved to a team of four people who manage the entirety of the globe that we were talking about. The 900 plus locations, 500,000 plus members, 10,000 plus employees, but while that sounds small, we act as really the quarterbacks, as I like to say, the quarterbacks during a crisis or an emergency.

What I mean by that is, even though there are only four of us on the global emergency management team, we are actually using force multipliers across the rest of enterprise risk management. We have colleagues in public affairs who we work closely with, colleagues in business continuity and disaster recovery, colleagues in information security and health and safety. So just there alone on the global scale, we're talking dozens of other people who we're working with, and on top of that, we have gone out and trained all of our leadership teams in every one of our territories, as we call them, our various, different countries or groups of countries, that are responsible for the day-to-day operations in our communities. And those folks, typically every territory has a team of anywhere between seven and 10 people. So we always have a force multiplier there that can help execute the actions that the risk management professionals need to have happen.

So even though a small enterprise or a risk management team on a global scale, we already have force multipliers, and we really play that quarterback or that conductor of an orchestra. We provide insights. We provide and remind people about our preplanned actions. One thing I always like to say, and I've stolen this from friends who work in the military, is that a plan is fantastic until it meets the reality of a crisis. It's at that point where the emergency management team comes in and starts saying, "All right, we had 10 steps that we needed to accomplish, but we know we can't accomplish five of them. How are we going to accomplish the other five because of the reality of the situation?" That's where I think our team really thrives.

Scott

Okay, thank you so much. Another question goes, earlier on in the presentation, you used the term blind spots and it's you're looking for the vulnerabilities, the risks. The question is, what are some good techniques that you've used that help your colleagues, help those other departments, see what the blind spots are?

Michael

It's a great question. I think the easiest way the first thing is to utilize technology as much as you can. We talked a lot about that in the webinar itself, and whether it's technology like Dataminr, whether it's technology such as traditional intelligence resources that comes to you through electronic means, provides you dashboards, those are great ways to start figuring out or start identifying threats that you haven't thought about.

Additionally, however, your blind spots, they're blind spots for a reason, right? You don't know what's out there. It's important as an enterprise risk manager, whether you're in emergency management or public affairs, to get to know the entirety of your business. One of the things that I pride our team on is, even if we're not the right person to execute an action, we know the right people to execute that action, and so risk management professionals need to be very gregarious, very outgoing, very much the social butterfly because, yes, a lot of people will say, "Oh, there comes the emergency management team. What's going to go wrong?"

But establish relationships with all the teams you can beforehand so that you can call on their expertise, have those subject matter experts in the room when you really need them. Doesn't matter, and I'll use an example that we had. When we first

had locations opening up in California and first had about two and a half years ago, real impact from wildfires occurring in California, not every team knew that we had engineers who could bring in air quality monitors into our spaces, right? That was a blind spot. We addressed that blind spot, we figured out which teams worked on those type of technologies and worked on those type of deployments of those kits, and now we know, okay, that blind spot might exist for someone who's brand new to the business, but when they say, "What do we do?" we already have the information in our back pocket. Sometimes it's a little bit of trial and error, but it's also about getting to know the rest of your business.

Scott

Okay, great. Next question. It's a Dataminr-specific question. How do you use Dataminr on a daily basis to evaluate risks beyond just data review?

Krista

Yeah, I mean, I don't know if it's how do you use it personally on a daily basis or from a risk perspective, and Michael is a user from a risk perspective. I use it daily for my general knowledge and knowledge of my clients and making sure that they're up to speed in getting all of the information that they need. But as far as from the risk perspective and receiving those notifications, I'll let Michael talk more about that from the user end.

Michael

What's really cool about Dataminr, specifically, is that it's insanely customizable, much more so than I've seen in other products we have as risk professionals. So, I'll use my team, for example. I am an information hog. I get all the information. I get hundreds of bits of information a day. That's not always easy to sort through, obviously, and it takes skill in doing that, but other parts of our security team and other parts of our risk teams use Dataminr in different ways. They scale back the information coming from Dataminr to their individual portfolios. We have Dataminr deployed for our security teams in, let's say, India, who are looking at information that only pertains to the buildings and the members that they have purview over.

How I use it beyond just a data dump is that when I see something, "Ooh, this might have the potential to turn into something." I was traveling this week and saw that there was a data point that came in through Dataminr about someone on a bus who said, "There is someone, looks like they're putting a vest that looks like it has explosives in it, on, on a bus." That bus was traveling in a city in which we have locations, and I said, "Okay, this might be something false, but I'm going to track this story, and I'm going to see it through to its conclusion because this could have an impact on our membership, depending where that bus goes. This could have an impact on our employees. This could have an impact on transportation."

So you have to use, this is where that combination of AI and your general awesome knowledge as a risk professional come together, and I think Krista would agree with this, is that this is supplementing, saying, "Okay, I, as a risk professional, see a threat. AI helped to identify it. Now, I have to think outside the box of just what the machine's telling me. How does this impact me specifically?" That's the greatest way that I use Dataminr is to start piquing my interests and running through potential scenarios. Obviously, you can't watch it 24/7 because the world is 24/7. It's a "sun never sets" model. But you have to ensure that you're at least using some kind of a platform to give you that edge that allows you to see beyond just what's in front of you or in your email or what you saw on the news at 6:00 a.m., because by 8:00 a.m., that data is no longer relevant.

Scott

Okay. We have another Dataminr question, a specific Dataminr question. How do you know who the employees and members around the event location in a given moment are, and how do you communicate with them in and avoid spamming people that are not there right now? So this is on following a Dataminr trigger. How do you know who the employees are? Go ahead.

Michael

Great question. So it really comes down to Dataminr is not going to tell you all the people in that particular location. We've imported all of our sites, all of our communities, into our Dataminr profiles to allow us to say, "Well, this is within a mile of this particular location." So that helps us start judging how far away do we care? How many sites are within the radius of this particular incident? So that initially helps us to avoid spamming people, but Dataminr is a information tool. It's not a broadcast tool, so we use a variety of other means to say, "Okay, the incident is happening according to Dataminr and according to our intelligence and according to other resources within a mile of five buildings in a city that has 20."

We already know that we can leave the 15 buildings alone and, if we're really smart, which we usually are, give those 15 buildings a different message saying, "Please do not go to this affected area because X is happening." So that gives us a way to only project information at the right time, to the right people in those 15 buildings. We can then focus on the 5 buildings. That is going to require you, as a risk manager, to again talk with multiple teams. If you don't have, in your particular team, access to your access control system records to know who's coming in and out of your buildings, you need to get in touch with the team who does. If you don't have access to the records of which members are in that location or in your corporate environment or which clients are at what particular location, you need to get with the team that does.

In our case, all of those teams are interconnected. Our member communications team helps us to know which members we target. Our directors of operations and our community teams who run the buildings, they let us know which employees are in those buildings. We also work with our Workday teams. We filter all of those through a variety of different broadcast messaging systems that allow us to very simply target people. Email's great, but if it's not targeted like the person who asked the question said, we are not going to give the right information to the right people at the right time, and here's the kicker, though. Inevitably, someone will say, "Don't tell me what to do," even if it's life-saving information or things that you, as a risk management team, think is life-saving, and you have to be prepared for that blowback. Doesn't mean that you spam someone, but if someone who's in London gets a message about what's happening in L.A., then you've failed. You have to be proactive and know which teams have access to which data to allow you to take a Dataminr alert and then properly message out the right people. It has to be cross-functional, again, multiple different technologies.

Scott

All right, that's great. I want to squeeze in one last question here, and it's this. What do you say to companies that do not see the value of implementing an enterprise risk management process? What are the strongest benefits that they can use to present to their executive management teams to argue the case that they need to start implementing an enterprise risk management process?

Michael

Very true. A very hard case to sometimes make, but here's the kicker, and I know we're running out of time. Essentially you have to say, "How is it that we did not ever

think to have an enterprise risk management team?" What crises have impacted your business that would have been better addressed by having an enterprise risk management team? It will take you a long time to make that case. It's taken us a long time to make that case, too. I'm not going to sugarcoat it and say, "Day one, suddenly we had an enterprise risk management team with all these interconnected teams across departments." That didn't happen.

It was about persevering and ensuring that your team kept doing whatever it was that you needed to do, whether you're crisis communications or enterprise risk management or emergency management. Building all your plans and cases, continuously building your use case scenario. It's not telling your executives, "Oh, well, remember when I told you that that storm was coming and we didn't do anything about it? Well, here's how we would've saved..." You don't want to rub their face in it and say, "You could've done better," but present them the case instead saying, "We know that this particular corporate location is in the path of hurricanes. In the past, we've had negative impacts, and in the past, we did not execute our plans as well as we could have. What we would like to propose is having a multi-departmental team together to address these risks going forward." Sometimes you have to use a negative event to help drive a long-term positive change in your enterprise. It is a question that many people have asked consistently, and there's no one solution to that problem, but it is about ensuring that you are doing the best job that you can for your company each and every time.

Scott All right. Thank you so much, Krista and Michael, for a great presentation today. This concludes today's webinar.